CLAIMS

1. A method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of application data units (ADUs);

b) encrypting the ADUs;

c) communicating the ADUs to a customer terminal;

d) in the locality of the customer terminal, decrypting the ADUs;

e) storing a record of the ADUs decrypted in step (d); and

f) subsequently generating a receipt for ADUs received at the customer terminal by reading record data stored in step (e) .

2. A method according to claim 1, in which the record stored in step (e) is generated by a secure module located at the customer terminal.

3. A method according to claim 2, in which the secure module encrypts the record and outputs it for storage outside the secure module

4. A method according to claim 2 ~~or 3~~ in which the encrypted ADUs are passed to the secure module, and the secure module outputs decrypted ADUs.

5. A method according to claim 1 ~~any one of the preceding claims~~, in which each of a plurality of ADUs output by the data source is encrypted with a different key, and a plurality of corresponding keys are generated at the customer terminal.

6. A method according to claim 5 when dependent on any one of claims 1 to 3, in which the secure module outputs the plurality of corresponding keys and the customer terminal uses the said keys to decrypt the plurality of ADUs.

7. A method according to claim 5 ~~or 6~~, in which the remote data source generates and communicates to the customer terminal a seed value and the plurality of different keys are generated from the said seed value.

8 A method according to claim 1 ~~any one of the preceding claims~~, including applying different characteristic variations to data decrypted at different respective customer terminals.

9. A method according to claim 8, in which the characteristic variation is applied after decryption of the data by a secure module.

10. A method according to claim 8, including generating a key for decryption of data, which key includes a characteristic variation, and the said characteristic variation in the in the data is induced by the characteristic variation in the key.

11. A method according to claim 1 ~~any one of the preceding claims~~ including returning the receipt to the server .

12. A data communications system comprising

a) a remote data source arranged to output a plurality of ADUs;

b) encryption means for encrypting the plurality of ADUs;

c) a communications network connected to the encryption means.

d) a customer terminal connected to the communications network and arranged to receive encrypted ADUs via the communications network;

e) decryption means located in the locality of the customer terminal and arranged to decrypt the ADUs received at the customer terminal from the communications network;

f) a store at the customer terminal for storing a record of ADUs decrypted by the decryption means;

g) means for reading record data from the store and generating thereby a receipt for ADUs received and decrypted by the customer terminal.

13. A data communications system according to claim 12, in which the communications network is a packet-switched network.

14. A data communications system according to claim 12 ~~or 13~~, in which a secure module in the customer terminal is arranged to generate the said record.

15. A data communications system according to claim 14, in which the secure module is arranged to encrypt the record

16. A data communications system according to claim 14 ~~or 15~~, in which the encryption means are arranged to encrypt different ADUs with different respective keys, and the secure module is arranged to generate a plurality of keys for decrypting the plurality of ADUs received at the customer terminal.

17. A customer terminal for use in a method according to ~~any one of claims 1 to 11~~ claim 1, the customer terminal comprising:

a) a data interface for receiving data from a data communications medium;

b) decryption means connected to the data interface and arranged to decrypt ADUs received via the data interface;

c) means for generating a record of ADUs decrypted by the decryption means; and

d) means for reading record data and generating thereby a receipt for ADUs received and decrypted by the decryption means.

18. A customer terminal according to claim 17, in which the means for generating a record is a secure module.

19. A customer terminal according to claim 16, in which the secure module is arranged to encrypt the record.

20. A customer terminal according to claim 18 ~~or 19~~ in which the secure module is arranged to generate a plurality of keys for decrypting the plurality of ADUs received at the customer terminal.

21. A method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of ADUs

b) encrypting different ones of the plurality of ADUs using different respective keys;

c) communicating ADUs to a customer terminal;

d) in the locality of the customer terminal, generating a plurality of different keys for decrypting different respective ADUs received at the customer terminal;

e) storing a record of the keys generated.

22. A data communications system comprising

a) a remote data source arranged to output a plurality of ADUs;

b) encryption means for encrypting the plurality of ADUs with different respective keys;

c) a communications network connected to the encryption means.

d) a customer terminal connected to the communications network and arranged to receive encrypted ADUs via the communications network;

e) a key generator programmed to generate a sequence of keys for use in decrypting ADUs:

f) decryption means connected to the key generator and arranged to decrypt the ADUs received at the customer terminal from the communications network; and

g) a store for storing a record of keys generated by the key generator means.

23. A customer terminal for use in a method according to claim 21, the customer terminal comprising:

a) a data interface for receiving data from a data communications medium;

b) a key generator programmed to generate a sequence of keys for use in decrypting ADUs:

c) decryption means connected to the data interface and to the key generator and arranged to decrypt ADUs received via the data interface;

d) a store containing a record of keys generated by the key generator; and

e) means for reading record data from the store and generating thereby a receipt for ADUs received and decrypted by the decryption means.

24. A method according to claim 1 ~~any one of claims 1 to 11 and 21~~, including generating keys from a seed value by iterated operations on the seed value by selected ones of a plurality of predetermined functions.

25. A method according to claim 24, in which the selection of the said predetermined functions is determined by the value of a ADU identity number.

26. A method according to 24 ~~or 25~~ in which the predetermined functions are computationally symmetric.

27. A method according to claim 26 in which the said functions are left-shifted binary XOR and right-shifted binary XOR.

28. A method of operating a data communications system comprising:

a) at a remote data source, outputting a plurality of application data units (ADUs) ;

b) encrypting the ADUs;

c) communicating the ADUs to a plurality of customer terminals;

d) in the locality of each customer terminal, decrypting the ADUs; and

e) inducing a different characteristic variation in the value of the ADU's at different respective terminals.

29. A method according to claim 28, in which the characteristic variation is applied after decryption of the data.

30. A method according to claim 28, including generating a key for decryption of data at a respective customer terminal, which key includes a characteristic variation, and the said characteristic variation in the in the ADU data is induced by the characteristic variation in the key.

31. A method according to ~~any one of claims 28 to 30~~ claim 28 further comprising:

f) reading decrypted ADU data; and

g) determining from the characteristic variations in the ADU data the identity of a terminal at which the said data was originally received.

32. A method or system according to ~~any one of the preceding claims~~ claim 28, in which ADU's are communicated to a customer terminal via a communications network.

33. A method or system according to any one of the preceding claims, including a plurality of remote data sources, each outputting a respective plurality of ADU's.

34. A method of operating a data communications system comprising:

a) at a plurality of remote data sources, outputting a plurality of application data units (ADUs) ;

b) encrypting the ADUs from different remote data sources with different respective keys derived from a common seed value;

c) communicating the ADUs to a plurality of customer terminals;

d) in the locality of each customer terminal, decrypting the ADU's.

35. A method or system according to claim 33 ~~or 34~~, in which the customer terminal receives a primary seed value common to different respective data streams from the plurality of data sources, and derives from the common primary key a plurality of different respective secondary seed values for decrypting ADU's from different respective data sources.

36. A method or system according to claim 35, in which data received from different data sources includes different respective source identity values, and the respective secondary seed value is generated from the primary seed value by modifying the primary seed value with the source identity value.